LAPORAN PRAKTIKUM

KEAMANAN INFORMASI 1

PERTEMUAN 5

(*IP and Enterprise Services Vulnerability*)

DISUSUN OLEH

Indah Sekar Ningrum (21/478139/SV/19241)

SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET

DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA

SEKOLAH VOKASI

UNIVERSITAS GADJAH MADA

YOGYAKARTA

2023

A. Menganalisis Log yang Ditangkap sebelumnya dan Pengambilan Lalu Lintas

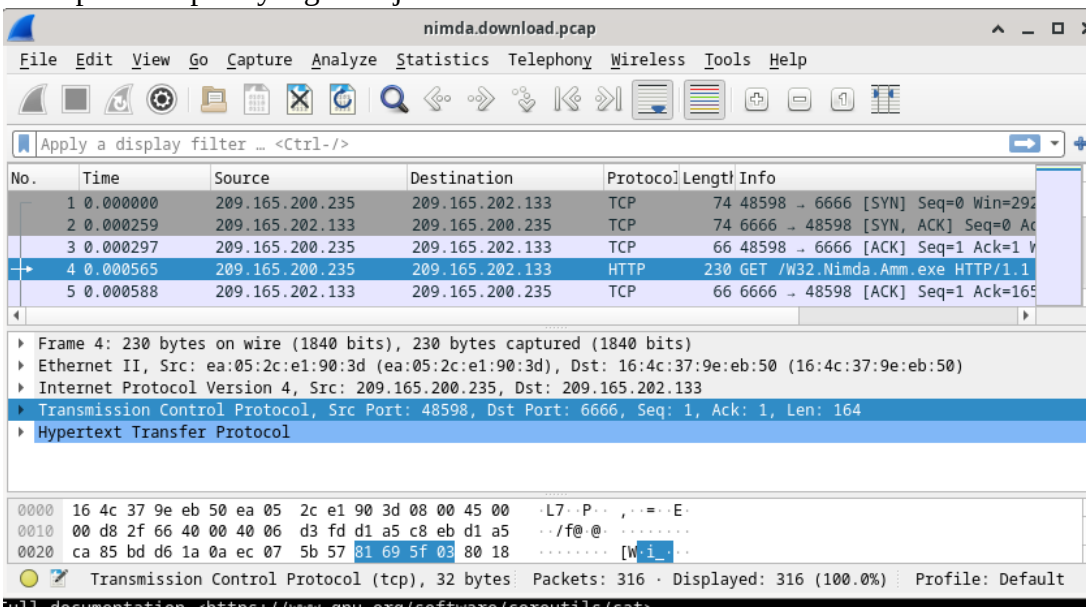
1. Ubah direktori ke folder lab.support.files/pcaps, dan dapatkan daftar file menggunakan perintah ls –l.

```
[analyst@secOps ~]$ ^C
[analyst@secOps ~]$ cd lab.support.files/pcaps
[analyst@secOps pcaps]$ ls -l
total 4028
-rw-r--r-- 1 analyst analyst  371462 Mar 21  2018 nimda.download.pcap
-rw-r--r-- 1 analyst analyst 3750153 Mar 21  2018 wannacry_download_pcap.pcap
```

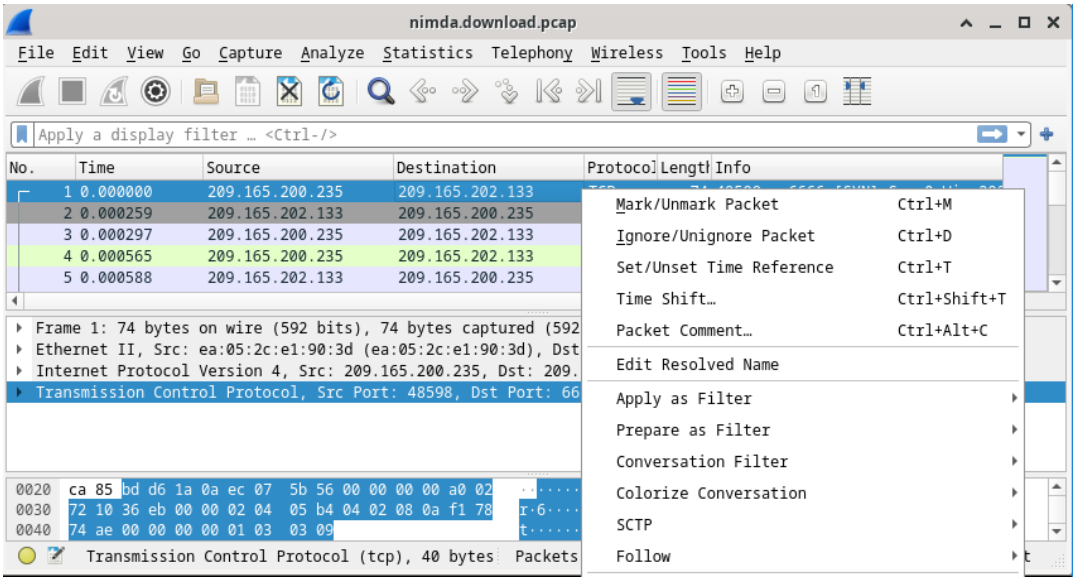
2. Keluarkan perintah di bawah ini untuk membuka file nimda.download.pcap di Wireshark.

```
[analyst@secOps pcaps]$ wireshark nimda.download.pcap &
[1] 2491
```

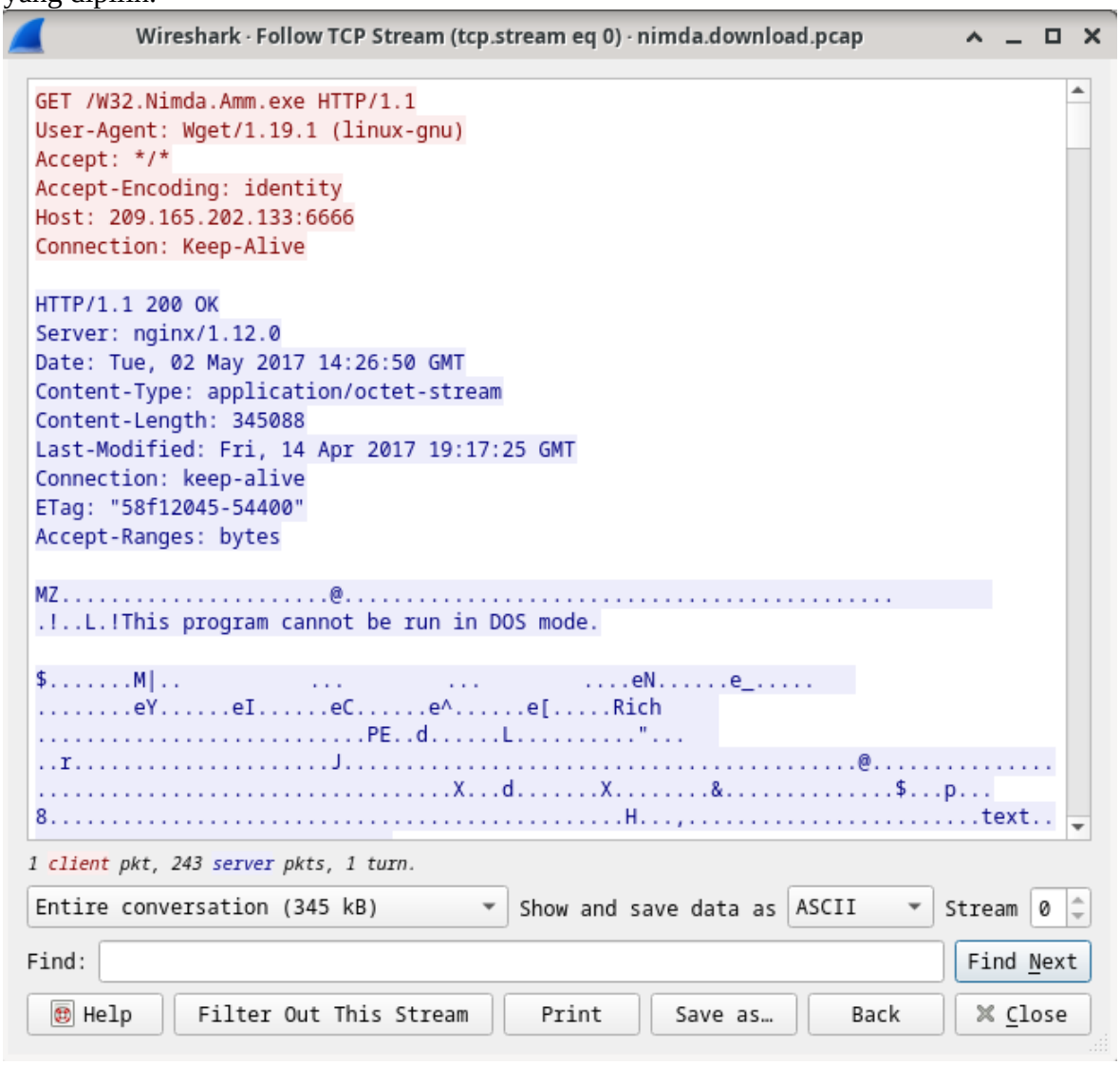
3. Pilih paket keempat dalam tangkapan dan perluas Protokol Transfer Hypertext untuk ditampilkan seperti yang ditunjukkan di bawah ini.



4. Pilih paket TCP pertama yang di capture, paket SYN. Klik kanan dan pilih Ikuti > TCP Stream.

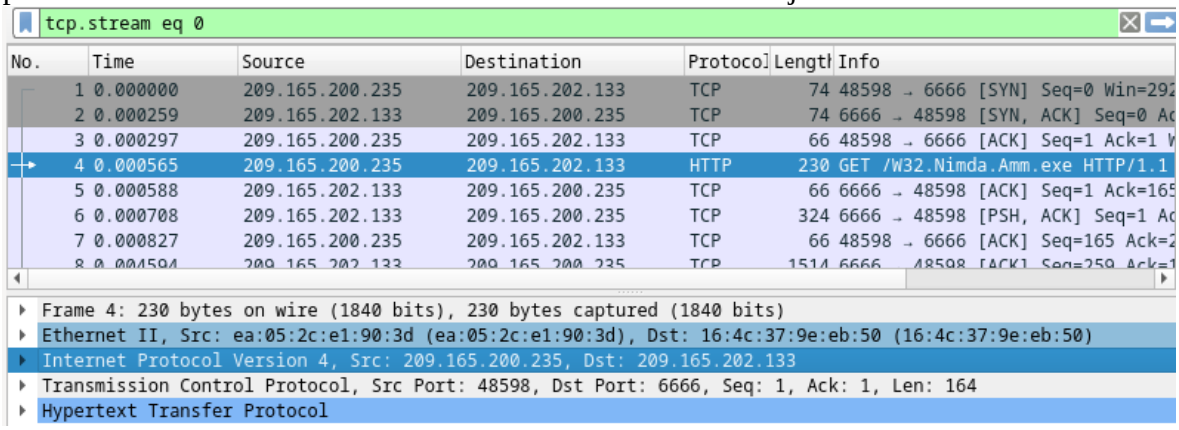


5. Wireshark menampilkan jendela lain yang berisi detail untuk seluruh aliran TCP yang dipilih.

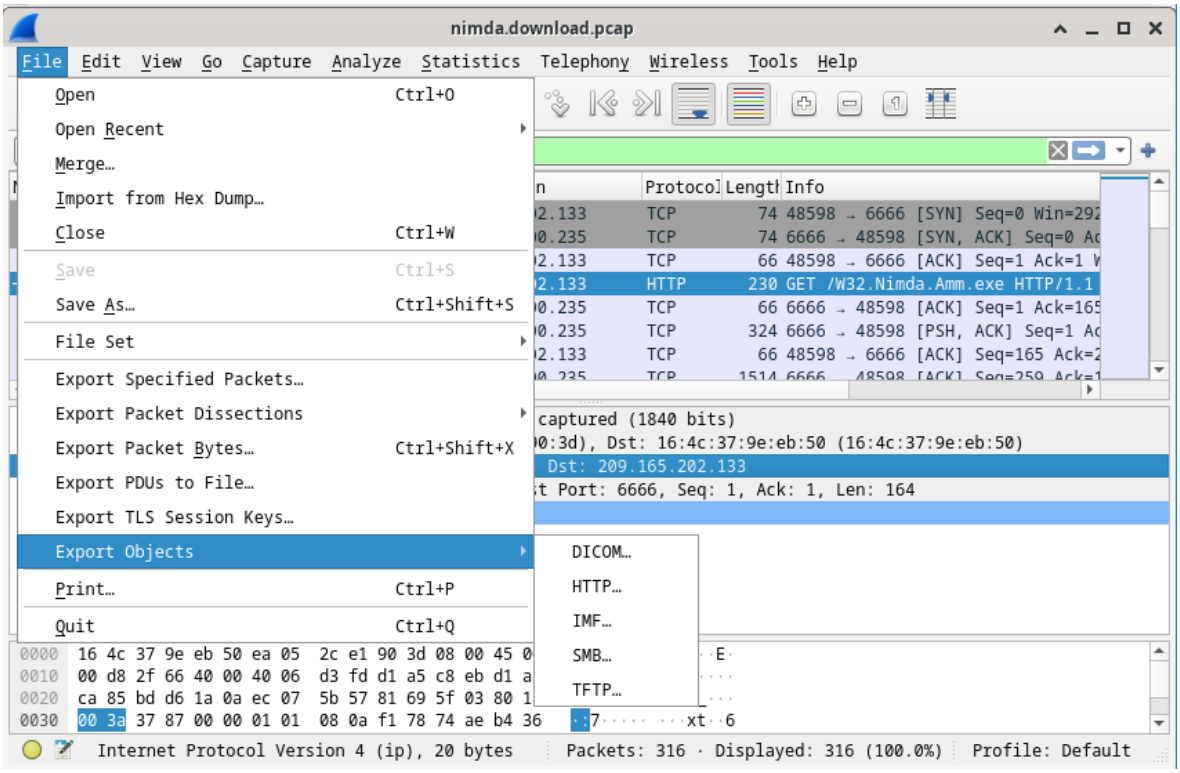


B. Extract Files yang di unduh dari PCAP

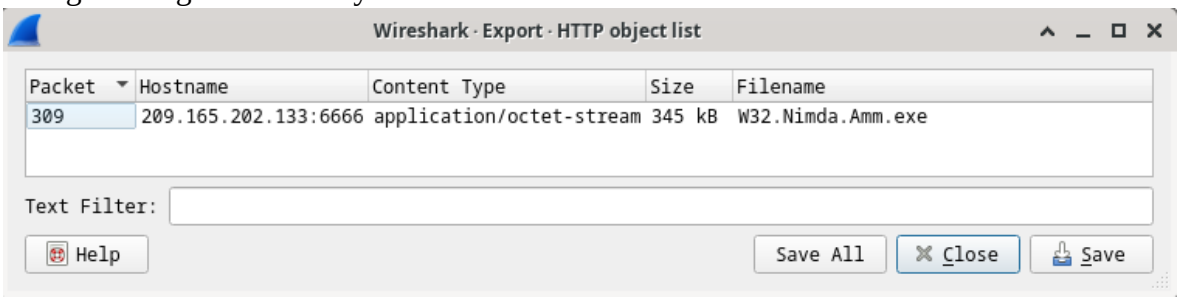
1. Dalam paket keempat dalam file nimda.download.pcap, perhatikan bahwa permintaan HTTP GET dihasilkan dari 209.165.200.235 menjadi 209.165.202.133.



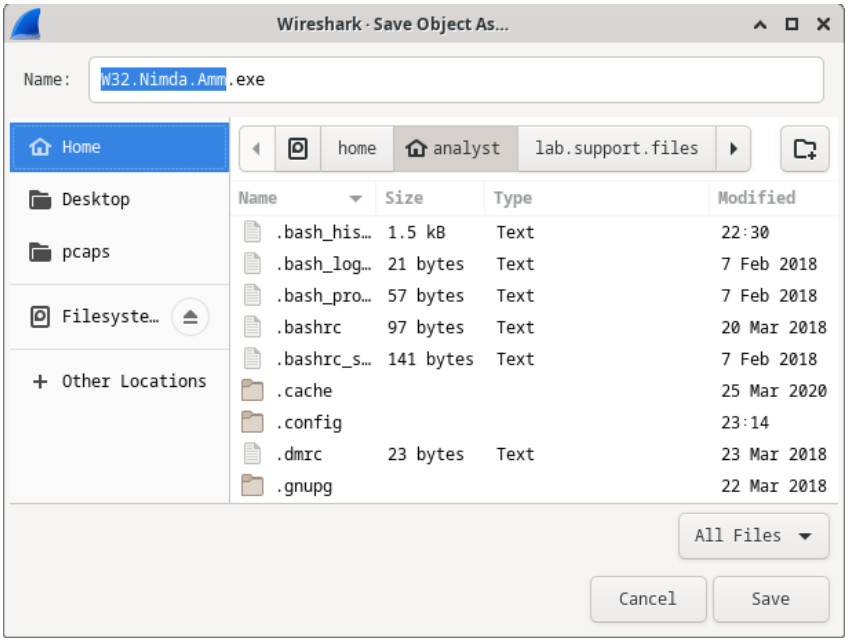
2. Navigasikan ke File > Export Objects > HTTP dari menu Wireshark



3. Wireshark akan menampilkan semua objek HTTP yang ada dalam aliran TCP yang berisi permintaan GET. Dalam hal ini, hanya file W32.Nimda.Amm.exe yang ada dalam pengambilan. Ini akan memakan waktu beberapa detik sebelum file ditampilkan.
4. Di jendela daftar objek HTTP, pilih file W32.Nimda.Amm.exe dan klik Simpan Sebagai di bagian bawah layar.



5. Klik panah kiri hingga Anda melihat tombol Beranda. Klik Beranda lalu klik folder analis (bukan tab analis). Simpan file di sana.



6. Kembali ke jendela terminal Anda dan pastikan file telah disimpan. Ubah direktori ke folder /home/analyst dan daftarkan file di folder tersebut menggunakan perintah ls -l.

```
[analyst@secOps ~]$ cd /home/analyst
[analyst@secOps ~]$ ls -l
total 380
drwxr-xr-x 2 analyst analyst   4096 May 20  2020 Desktop
drwxr-xr-x 3 analyst analyst   4096 Apr  2  2020 Downloads
-rw-r--r-- 1 root    root     16557 Feb 20 21:51 httpdump.pcap
-rw-r--r-- 1 root    root        24 Feb 20 21:45 httpsdump.pcap
drwxr-xr-x 9 analyst analyst   4096 Jul 15  2020 lab.support.files
drwxr-xr-x 2 analyst analyst   4096 Mar 21  2018 second_drive
-rw-r--r-- 1 analyst analyst 345088 Feb 20 23:14 W32.Nimda.Amm.exe
```

7. Perintah file memberikan informasi tentang jenis file. Gunakan perintah file untuk mempelajari lebih lanjut tentang malware, seperti yang ditunjukkan di bawah ini:

```
[analyst@secOps ~]$ file W32.Nimda.Amm.exe
W32.Nimda.Amm.exe: PE32+ executable (console) x86-64, for MS Windows
```

A. Security Onion VM.

Luncurkan Security Onion VM dari Dasbor VirtualBox (username: analyst / password: cyberops).

B. Zeek Logs pada Security Onion

1. Dari jendela terminal, ubah direktori menggunakan perintah berikut.

```
analyst@SecOnion:~$ cd /nsm/bro/logs/current
analyst@SecOnion:/nsm/bro/logs/current$
```

2. Gunakan perintah ls -l untuk melihat file log yang dihasilkan oleh Zeek:

```
analyst@SecOnion:/nsm/bro/logs/current$ ls -l
total 0
```

C. Snort Logs

1. Log snort dapat ditemukan di /nsm/sensor_data/. Ubah direktori sebagai berikut.

```
analyst@SecOnion:/nsm/bro/logs/current$ cd /nsm/sensor_data
analyst@SecOnion:/nsm/sensor_data$
```

2. Gunakan perintah ls -l untuk melihat semua file log yang dihasilkan oleh Snort.

```
analyst@SecOnion:/nsm/sensor_data$ ls -l
total 12
drwxrwxr-x 7 sguil sguil 4096 Jun 19  2020 seconion-eth0
drwxrwxr-x 5 sguil sguil 4096 Jun 19  2020 seconion-eth1
drwxrwxr-x 7 sguil sguil 4096 Jun 19  2020 seconion-import
```

3. Gunakan perintah ls –l seconion-eth0 untuk melihat file yang dihasilkan oleh antarmuka eth0.

```
analyst@SecOnion:/nsm/sensor_data$ ls -l seconion-eth0
total 28
drwxrwxr-x 2 sguil sguil 4096 Jun 19  2020 argus
drwxrwxr-x 3 sguil sguil 4096 Jun 19  2020 dailylogs
drwxrwxr-x 2 sguil sguil 4096 Jun 19  2020 portscans
drwxrwxr-x 2 sguil sguil 4096 Jun 19  2020 sancp
drwxr-xr-x 2 sguil sguil 4096 Jun 19  2020 snort-1
-rw-r--r-- 1 sguil sguil 5594 Jun 19  2020 snort-1.stats
-rw-r--r-- 1 root  root     0 Jun 19  2020 snort.stats
```

D. Various Logs

1. Sementara direktori /nsm/ menyimpan beberapa file log, file log yang lebih spesifik dapat ditemukan di bawah /var/log/nsm/. Ubah direktori dan gunakan perintah ls untuk melihat semua file log di direktori.

```
analyst@SecOnion:/nsm/sensor_data$ cd /var/log/nsm/
analyst@SecOnion:/var/log/nsm$ ls
eth0-packets.log        sensor-newday-argus.log
netsniff-sync.log       sensor-newday-http-agent.log
ossec_agent.log         sensor-newday-pcap.log
seconion-eth0           so-elastic-configure-kibana-dashboards.log
seconion-import         so-elasticsearch-pipelines.log
securityonion           sosetup.log
sensor-clean.log        so-zeek-cron.log
sensor-clean.log.1.gz   squert-ip2c-5min.log
sensor-clean.log.2.gz   squert-ip2c.log
sensor-clean.log.3.gz   squert_update.log
sensor-clean.log.4.gz   watchdog.log
sensor-clean.log.5.gz   watchdog.log.1.gz
sensor-clean.log.6.gz   watchdog.log.2.gz
sensor-clean.log.7.gz   watchdog.log.3.gz
```

2. Log ELK dapat ditemukan di direktori /var/log. Ubah direktori dan gunakan perintah ls untuk membuat daftar file dan direktori.

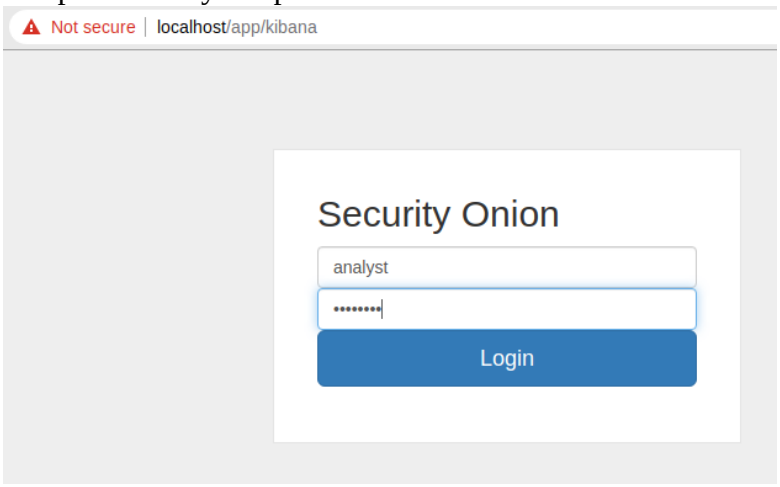
```
analyst@SecOnion:/var/log/nsm$ cd ..
analyst@SecOnion:/var/log$ ls
alternatives.log        daemon.log.1      gpu-manager.log  samba
alternatives.log.1      daemon.log.2.gz   installer        sguild
alternatives.log.2.gz   daemon.log.3.gz   kern.log         so-boot.log
alternatives.log.3.gz   daemon.log.4.gz   kern.log.1       syslog
alternatives.log.4.gz   debug             kern.log.2.gz    syslog.1
apache2                 debug.1           kibana           syslog.2.gz
apt                     debug.2.gz        lastlog          syslog.3.gz
auth.log                debug.3.gz        lightdm          syslog.4.gz
auth.log.1              debug.4.gz        logstash         syslog.5.gz
auth.log.2.gz           dmesg             lpr.log          syslog.6.gz
auth.log.3.gz           domain_stats      mail.err         syslog.7.gz
auth.log.4.gz           dpkg.log          mail.info        unattended-upgrades
boot                    dpkg.log.1        mail.log         user.log
boot.log                elastalert        mail.warn        user.log.1
bootstrap.log           elasticsearch     messages         user.log.2.gz
btmp                    error             messages.1       user.log.3.gz
btmp.1                  error.1           messages.2.gz    user.log.4.gz
cron.log                error.2.gz        messages.3.gz    wtmp
cron.log.1              error.3.gz        messages.4.gz    wtmp.1
cron.log.2.gz           error.4.gz        mysql            Xorg.0.log
cron.log.3.gz           faillog           nsm              Xorg.0.log.old
cron.log.4.gz           freq_server       ntpstats         Xorg.1.log
curator                 freq_server_dns   redis
daemon.log              fsck              salt
```

A. Ubah jangka waktu /timeframe

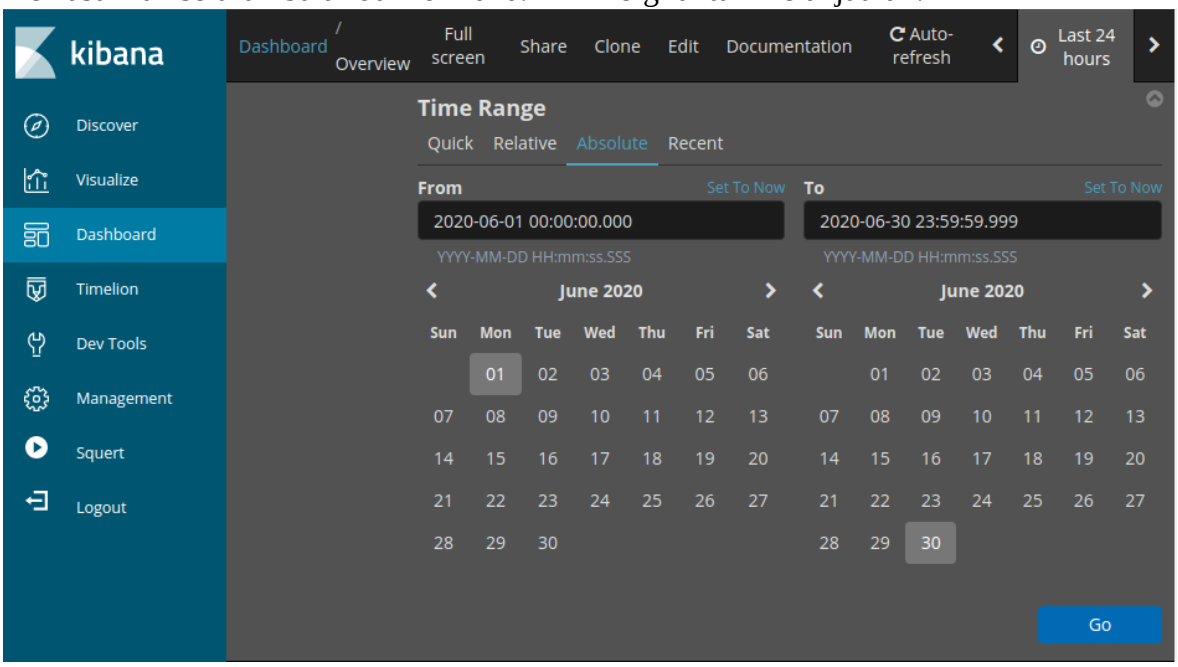
1. Mulai Security Onion VM dan masuk dengan username analyst and the password cybercops.
2. Masukkan perintah sudo so-status untuk memeriksa status layanan. Status untuk semua layanan harus OK sebelum memulai analisis . Ini bisa memakan waktu beberapa menit.

```
analyst@SecOnion:/$ sudo so-status
[sudo] password for analyst:
Status: securityonion
  * sguil server                                                    [  OK  ]
Status: seconion-import
  * pcap_agent (sguil)                                              [  OK  ]
  * snort_agent-1 (sguil)                                           [  OK  ]
  * barnyard2-1 (spooler, unified2 format)                          [  OK  ]
Status: Elastic stack
  * so-elasticsearch                                                [  OK  ]
  * so-logstash                                                     [  OK  ]
  * so-kibana                                                       [  OK  ]
  * so-freqserver                                                   [  OK  ]
```

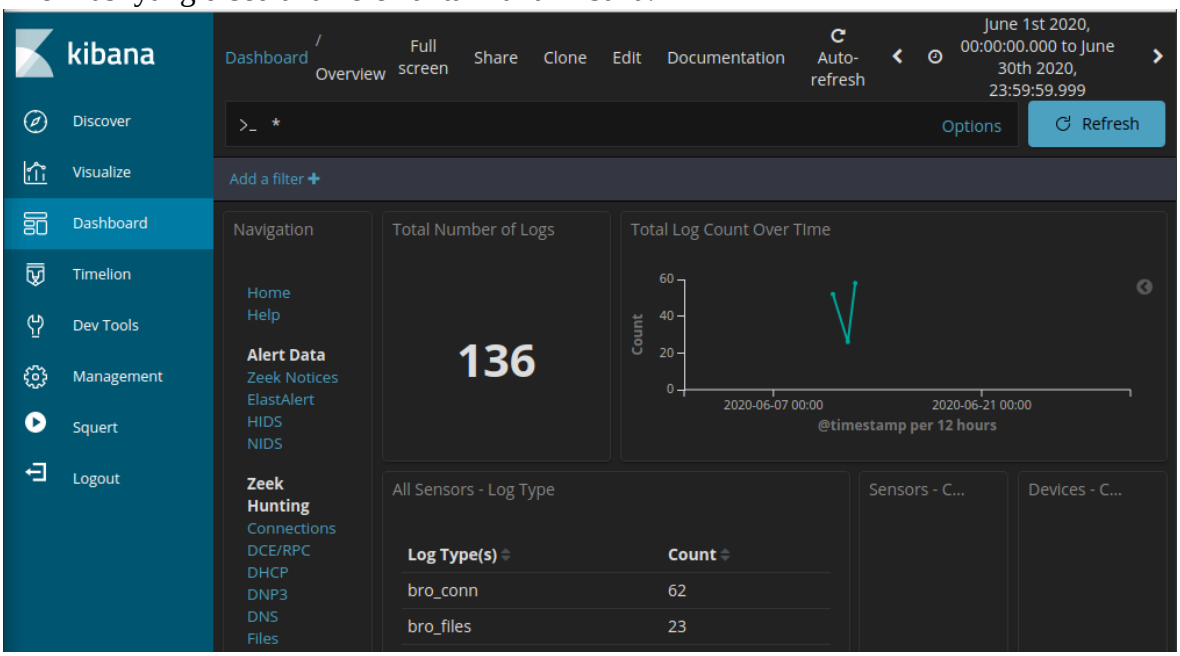
3. Buka Kibana menggunakan pintasan di Desktop. Masuk dengan username analyst dan password cyberops.



4. Di sudut kanan atas jendela, klik 24 jam terakhir untuk mengubah ukuran Rentang Waktu sampel. Perluas rentang waktu untuk menyertakan peringatan yang menarik. Serangan injeksi SQL terjadi pada Juni 2020 jadi itulah yang perlu Anda targetkan. Pilih Absolute di bawah Rentang Waktu dan edit waktu Dari dan Ke untuk memasukkan seluruh bulan Juni di 2020. Klik Pergi untuk melanjutkan.

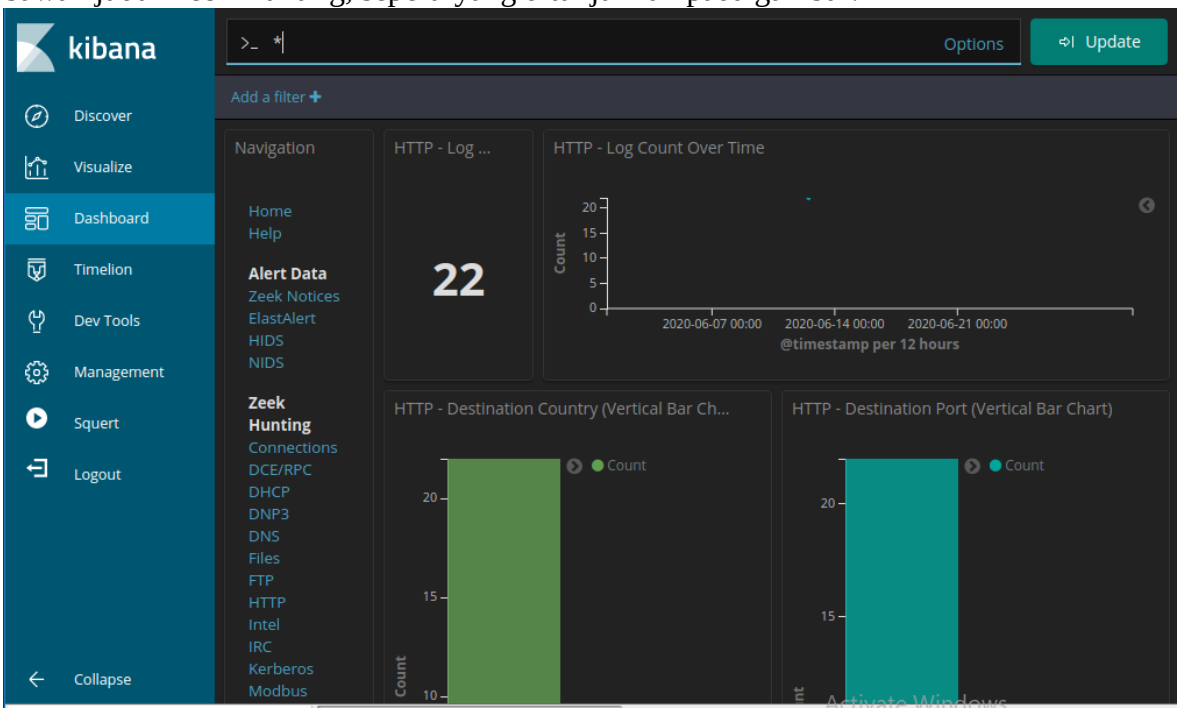


5. Perhatikan jumlah total log untuk seluruh bulan Juni 2020. Dasbor Anda harus serupa dengan yang ditunjukkan pada gambar. Luangkan waktu sejenak untuk menjelajahi informasi yang disediakan oleh antarmuka Kibana.

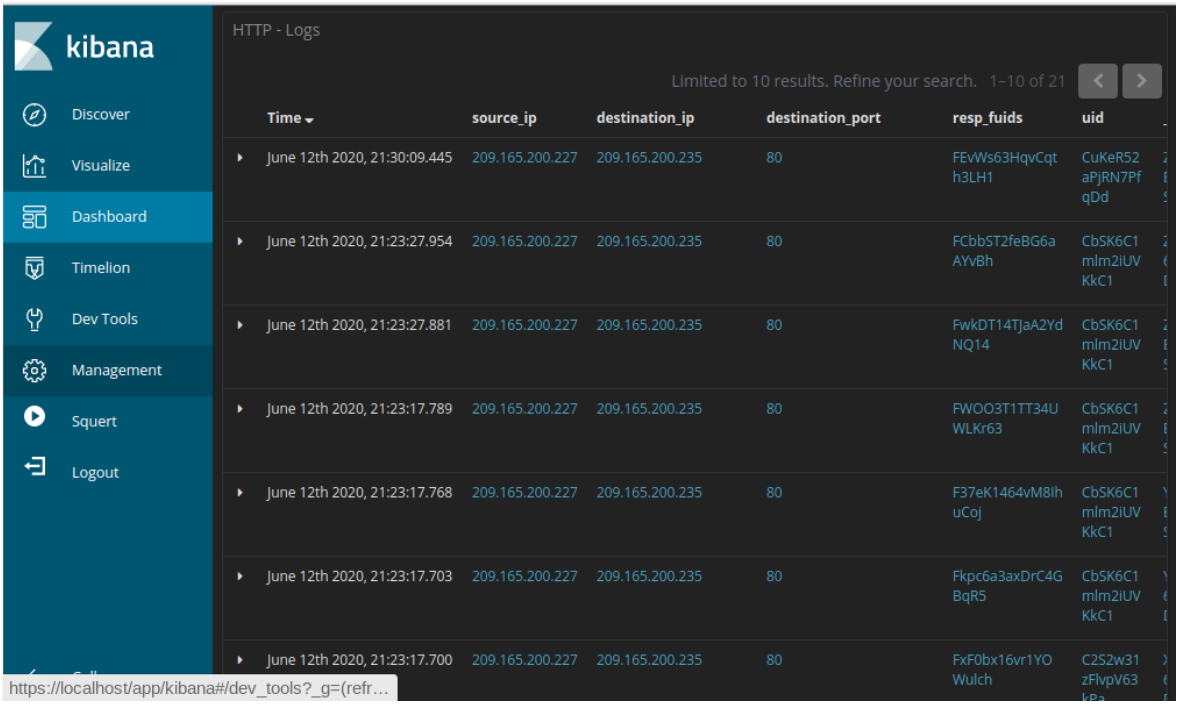


B. Filter dari HTTP traffic

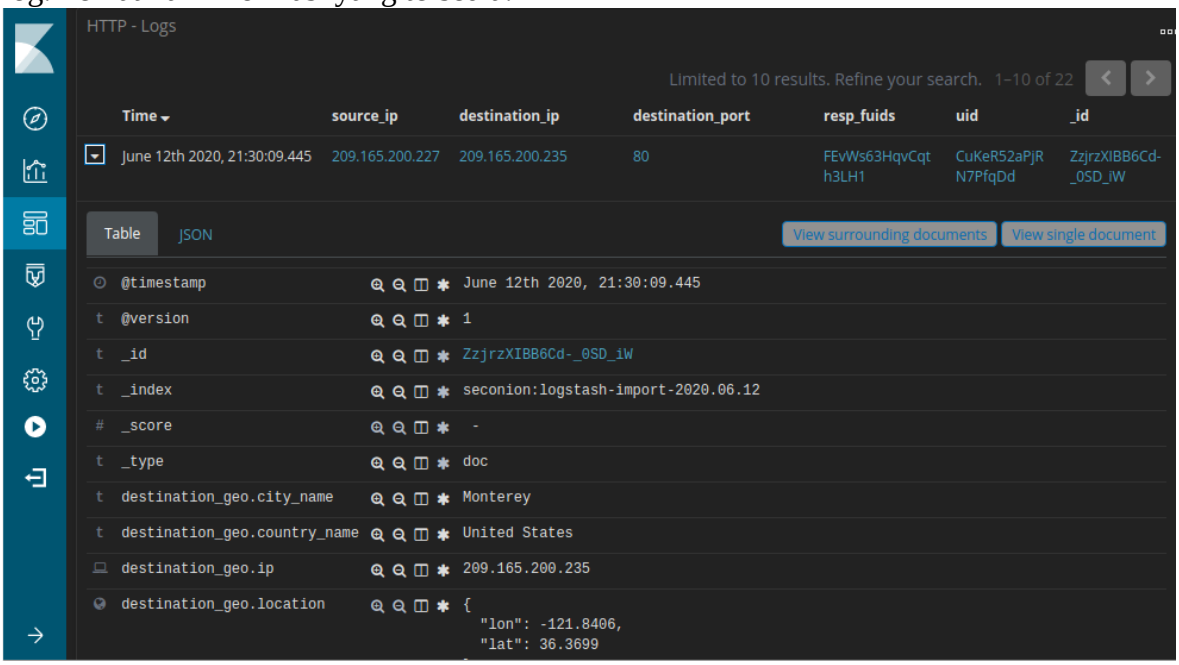
6. Karena aktor ancaman menilai data yang disimpan di server web, filter HTTP digunakan untuk memilih log yang terkait dengan lalu lintas HTTP. Pilih HTTP di bawah judul Zeek Hunting, seperti yang ditunjukkan pada gambar.



7. Gulir ke bawah ke Log HTTP. daftar 10 hasil pertama.



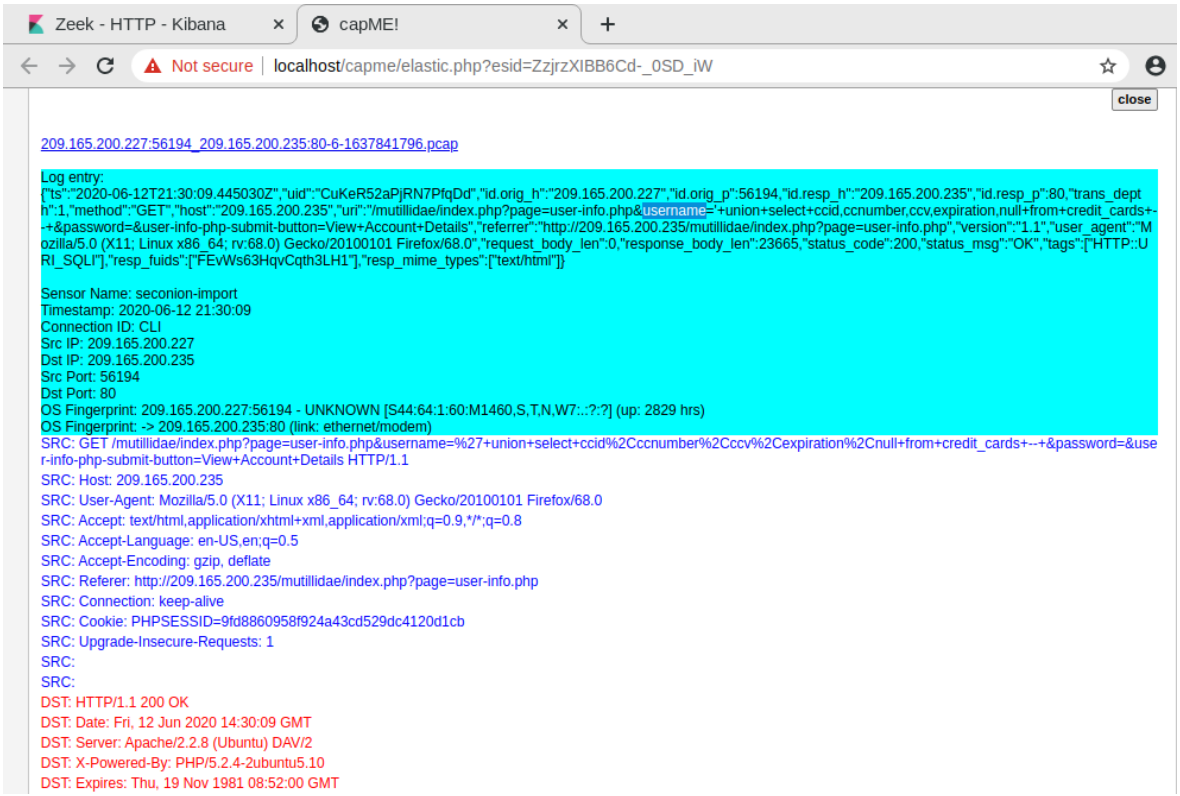
8. Klik detail hasil pertama dengan mengklik panah yang ada di sebelah timestamp entri log. Perhatikan informasi yang tersedia.



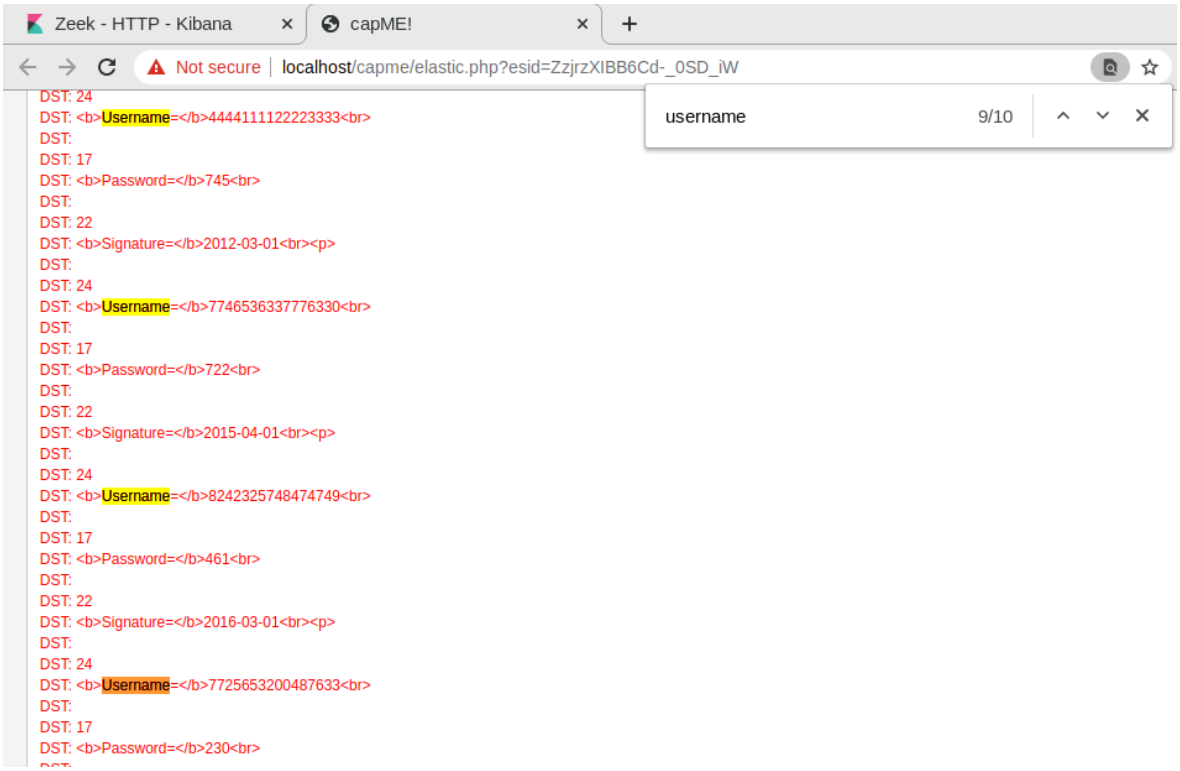
C. Review hasil

9. Beberapa informasi untuk entri log ditautkan ke alat lain. Klik nilai di bidang alert _id dari entri log untuk mendapatkan tampilan yang berbeda pada event tersebut.
10. Hasilnya terbuka di tab browser web baru dengan informasi dari capME!. capME! tab adalah antarmuka web yang memungkinkan Anda melihat transkrip pcap. Teks biru berisi permintaan HTTP yang dikirim dari sumber (SRC). Teks merah adalah tanggapan dari server web tujuan (DST).
11. Di bagian entri Log, yang ada di awal transkrip, perhatikan bagian username='+union+select+ccid,ccnumber,ccv,expiration,null+from+credit_cards+-

-+&password= menunjukkan bahwa seseorang mungkin telah mencoba untuk menyerang browser web menggunakan injeksi SQL untuk melewati otentikasi. Kata kunci, union dan select, adalah perintah yang digunakan dalam mencari informasi dalam database SQL. Jika kotak input pada halaman web tidak terlindungi dengan baik dari input ilegal, pelaku ancaman dapat menyuntikkan string pencarian SQL atau kode lain yang dapat mengakses data yang terdapat dalam database yang ditautkan ke halaman web.

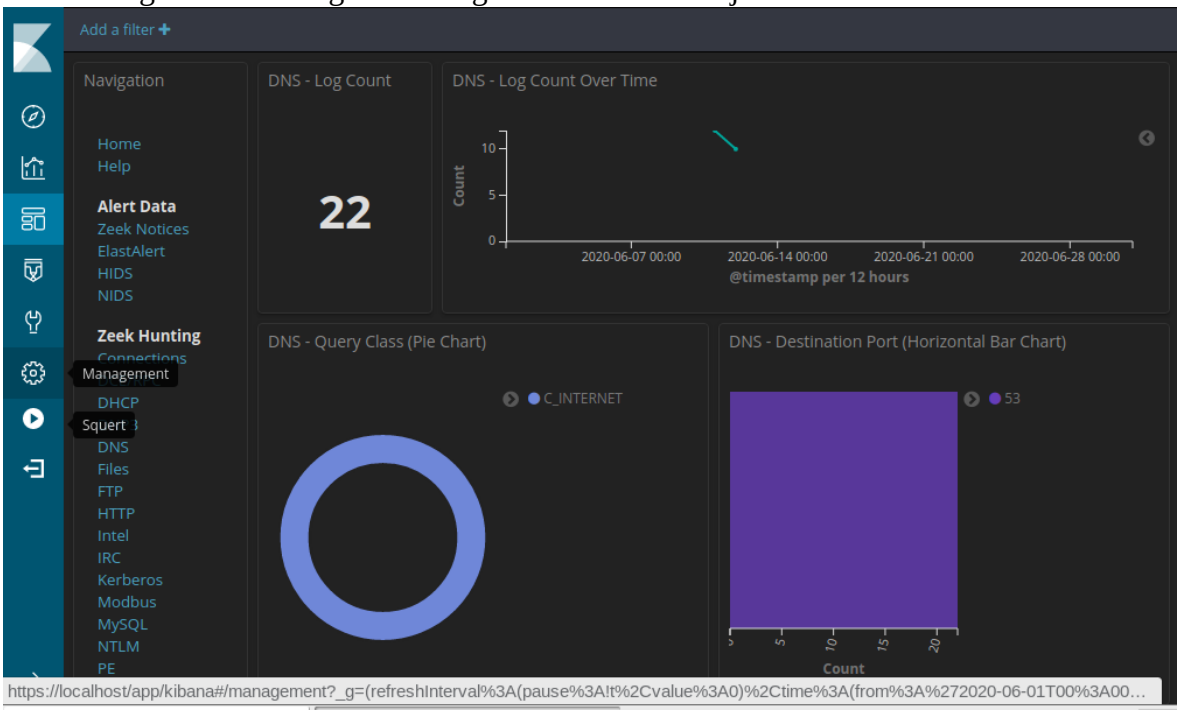


12. Temukan keyword nama pengguna dalam transkrip. Gunakan Ctrl-F untuk membuka kotak pencarian. Gunakan tombol panah bawah di kotak pencarian untuk menelusuri kejadian yang ditemukan.



D. Filter DNS traffic

13. Dari bagian atas Dasbor Kibana, hapus semua filter dan istilah pencarian dan klik Beranda di bawah bagian Navigasi Dasbor. Periode Waktu masih harus mencakup Juni 2020.
14. Di area Dashboard yang sama, klik DNS di bagian Zeek Hunting. Perhatikan metrik Jumlah Log DNS dan diagram batang horizontal Port Tujuan.

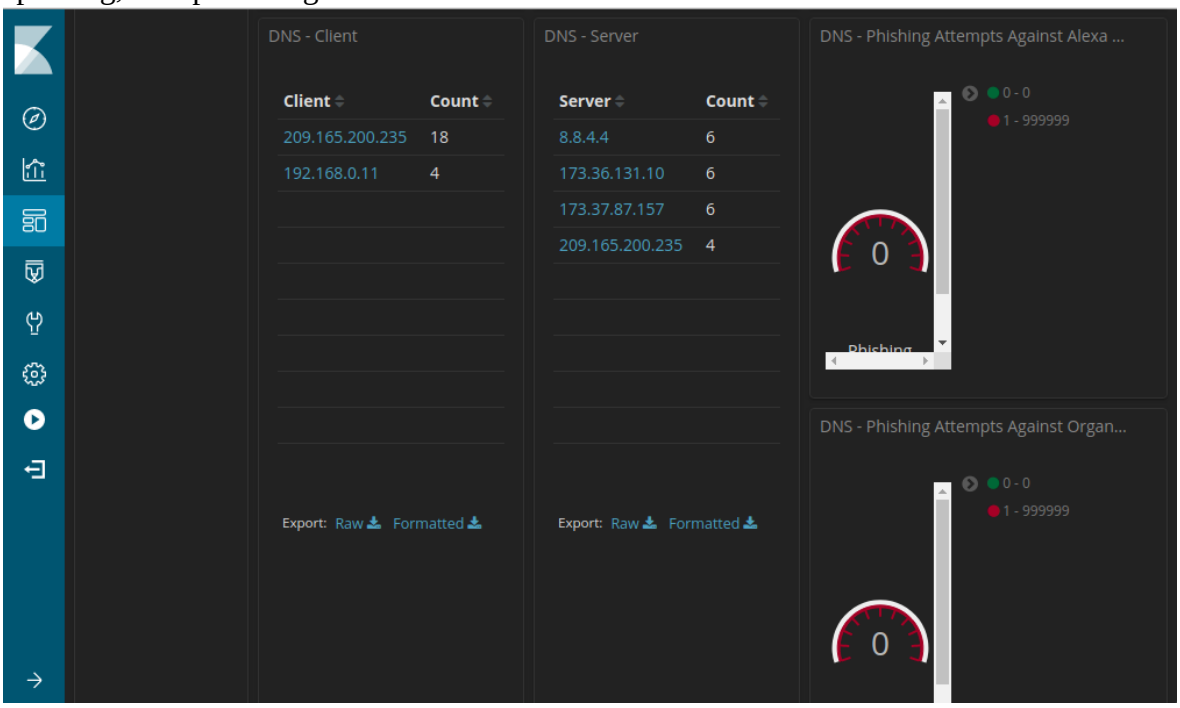


E. Tinjau entri terkait DNS

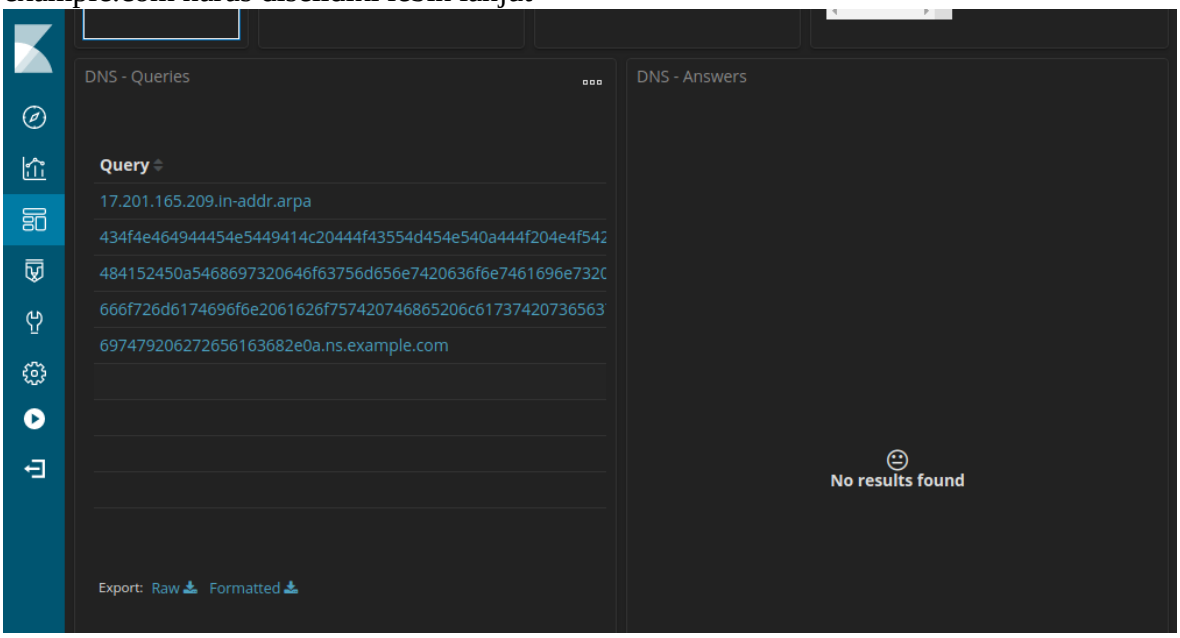
15. Gulir ke bawah jendela. Anda dapat melihat jenis kueri DNS teratas. Anda mungkin melihat catatan alamat (catatan A), alamat IPv6 catatan Quad A (AAAA), catatan

NetBIOS (NB) dan catatan pointer untuk menyelesaikan nama host (PTR). Anda juga dapat melihat kode respons DNS.

16. Dengan Menggulir lebih jauh ke bawah, Anda dapat melihat daftar klien DNS dan Server DNS teratas berdasarkan jumlah permintaan dan respons mereka. Ada juga metrik untuk jumlah upaya DNS Phishing, yang juga dikenal sebagai pharming DNS, spoofing, atau poisoning.

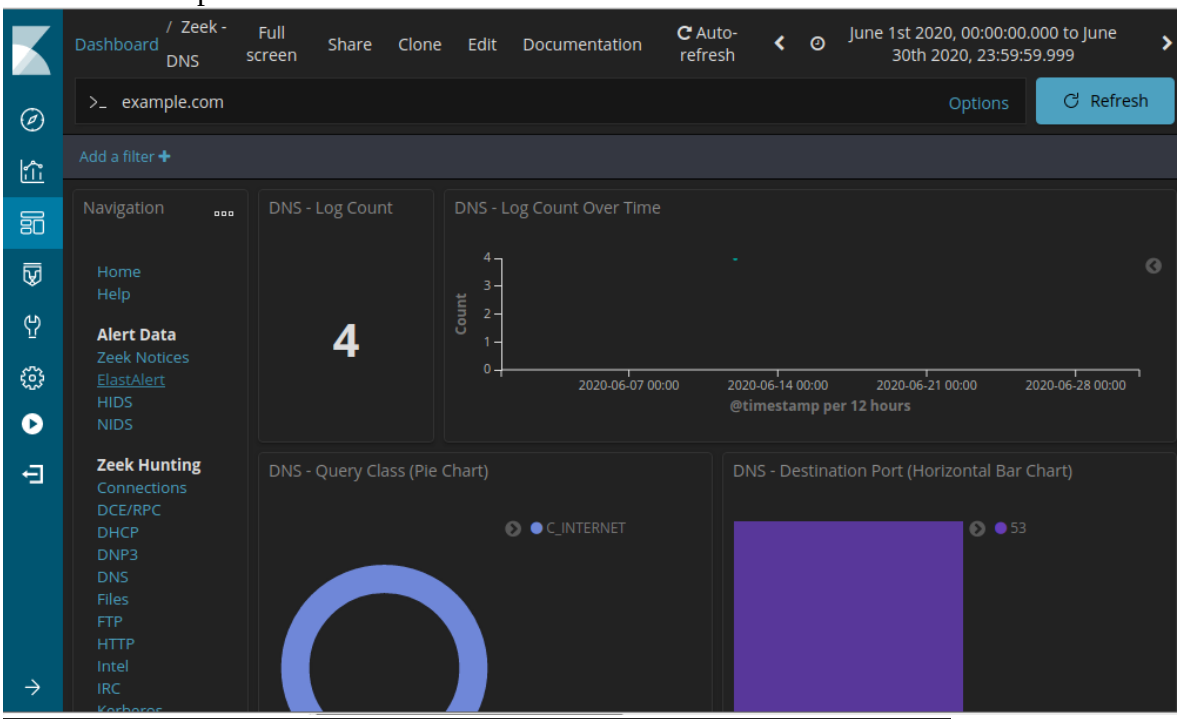


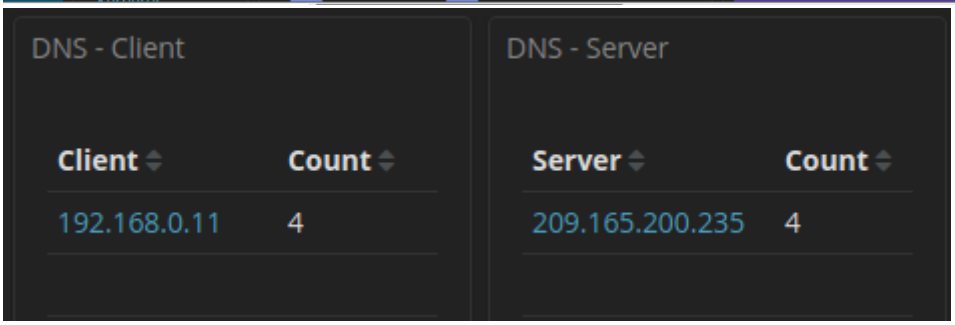
17. Menggulir lebih jauh ke bawah jendela, Anda dapat melihat daftar kueri DNS teratas berdasarkan nama domain. Perhatikan bagaimana beberapa kueri memiliki subdomain yang sangat panjang yang dilampirkan ke ns.example.com. Domain example.com harus diselidiki lebih lanjut



18. Gulir kembali ke bagian atas jendela dan masukkan example.com di bilah pencarian untuk memfilter example.com dan klik Perbarui. Perhatikan bahwa jumlah entri

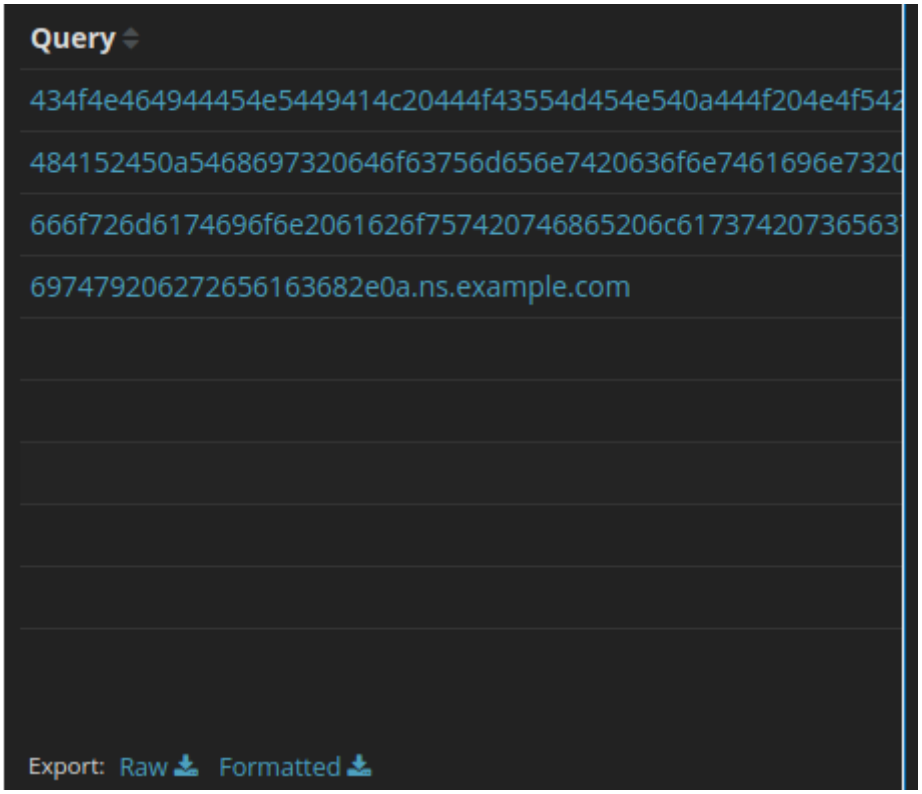
dalam Hitungan Log lebih kecil karena tampilan sekarang terbatas pada permintaan ke server example.com.





F. Tentukan data yang diekstraksi

19. Lanjutkan untuk menggulir lebih jauh ke bawah untuk melihat empat entri log unik untuk kueri DNS ke example.com. Perhatikan bagaimana kueri ke subdomain panjang yang mencurigakan yang dilampirkan ke ns.example.com. String panjang angka dan huruf di subdomain terlihat seperti teks yang dikodekan ke dalam heksadesimal (0-9, a-f) daripada nama subdomain yang sah. Klik tautan Ekspor: Unduh untuk mengunduh kueri ke file eksternal. File CSV diunduh ke folder /home/analyst/Downloads.



20. Arahkan ke folder /home/analyst/Downloads. Buka file menggunakan editor teks, seperti gedit. Edit file dengan menghapus teks di sekitar bagian heksadesimal dari subdomain, hanya menyisakan karakter heksadesimal. Pastikan untuk menghapus tanda kutip juga. Isi file Anda akan terlihat seperti informasi di bawah ini. Simpan file teks yang diedit dengan nama file asli.

21. Di terminal, gunakan perintah xxd untuk memecahkan kode teks dalam file CSV dan menyimpannya ke file bernama secret.txt. Gunakan cat untuk menampilkan konten secret.txt ke konsol.